This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1.-14. (Canceled)

15. (Currently Amended) A method for a secure processor to instantiate and authenticate a secure application thereon by way of a security kernel, the method comprising:

powering on into a normal mode;

receiving an instruction to instantiate the application after being powered on and while being in the normal mode;

after receiving the instruction to instantiate the application, transitioning from the normal mode to ~~entering~~ a preferred mode upon a non-power-up executed CPU reset, where a security key of the processor is accessible while in the preferred mode;

instantiating and running a security kernel while in the preferred mode, the security kernel:

accessing the security key;

applying the accessed security key to decrypt at least one encrypted key for the application;

storing the decrypted key(s) in a location where the application will expect the key(s) to be found; and

authenticating the application on the processor;

instantiating the application while in the preferred mode and only after the security kernel has authenticated such application; and

transitioning from the preferred mode to the ~~entering a~~ normal mode ~~from the preferred mode~~ after the security kernel authenticates the application and the application has been instantiated, where the security key is not accessible while in the normal mode, the application as instantiated during the preferred mode being available for use during the transitioned-to normal mode;

wherein the security kernel allows the processor to be trusted to keep hidden the security key(s) of the application, and

wherein the security kernel employs the accessed security key during the preferred mode to authenticate / verify the application prior to instantiation thereof~~,~~

~~wherein the processor has a cache, the method further comprising .~~

~~erasing data in the cache of the processor when entering preferred mode such that any data previously stored in the cache is not available to interfere with preferred mode operations; and~~

~~erasing data in the cache of the processor when entering normal mode such that any sensitive data in the cache from preferred mode operations is not available during normal mode from such cache~~.

16.-19. (Canceled)

20. (Previously Presented) The method of claim 15 wherein the security kernel performs a hash / MAC (message authentication code) over at least a portion of the application and then compares the hash / MAC to a hash / MAC corresponding to the application.

21. (Original) The method of claim 15 wherein the security key of the processor is a symmetric key and the application is instantiated from a code image including a main body and a header including:

KCPU (KMAN)	KMAN encrypted according to KCPU
KMAN (KCODE)	KCODE encrypted according to KMAN

where KCPU is the security key, KMAN is a device key of the portable device independent of the security key, and KCODE is the secret of the application, and

wherein the security kernel applying the accessed security key to decrypt at least one encrypted key for the application comprises:

applying KCPU to KCPU (KMAN) to produce KMAN; and

applying KMAN to KMAN (KCODE) to produce KCODE.

22. (Original) The method of claim 21 wherein the security key of the processor is a symmetric key and the application is instantiated from a code image including a main body and a header including:

KCPU (KMAN)	KMAN encrypted according to KCPU
MAC (main body, KMAN)	message authentication code of the main body under KMAN
KMAN (KCODE)	KCODE encrypted according to KMAN

where KCPU is the security key, KMAN is a device key of the portable device independent of the security key, and KCODE is the secret of the application, and

wherein the security kernel applying the accessed security key to decrypt at least one encrypted key for the application comprises:

applying KCPU to KCPU (KMAN) to produce KMAN;

computing MAC (main body, KMAN);

comparing the computed MAC to MAC (main body, KMAN) from the header to determine if the code image has been changed; and

if the MACs match, applying KMAN to KMAN (KCODE) to produce KCODE.

23. (Original) The method of claim 15 wherein the security key of the processor is a private key of a public key - private key pair and the application is instantiated from a code image including a main body and a header including:

public key (KCODE)	KCODE encrypted according to the public key

where KCODE is the secret of the application, and

wherein the security kernel applying the accessed security key to decrypt at least one encrypted key for the application comprises applying the security key as the private key to public key (KCODE) to produce KCODE.

24. (Original) The method of claim 23 wherein the security key of the processor is a private key of a public key - private key pair and the application is instantiated from a code image including a main body and a header including:

public key (HASH (main body), KCODE)	Hash of the main body and KCODE, both encrypted according to the public key

where KCODE is the secret of the application, and

wherein the security kernel applying the accessed security key to decrypt at least one encrypted key for the application comprises:

computing HASH (main body);

applying the private key to public key (HASH (main body), KCODE) to produce HASH (main body) and KCODE;

comparing the computed HASH to the produced HASH to determine if the code image has been changed;; and

if the HASHs match, employing the produced KCODE as appropriate.

25. (Currently Amended) A method for a secure processor to instantiate one of a plurality of available secure applications thereon by way of a security kernel, the method comprising:

setting a chooser value to a value corresponding to a chooser application upon power-up;

entering a preferred mode upon a first power-up CPU reset and instantiating and running the security kernel while in a preferred mode, the security kernel determining that the chooser value corresponds to the chooser application and therefore authenticating same, the chooser application being instantiated by the security kernel while in the preferred mode and only after being authenticated;

transitioning from the preferred mode to a ~~entering a~~ normal mode after the chooser application is instantiated and leaving same to run while in the normal mode, the

chooser application while in the normal mode presenting the plurality of available applications for selection by a user;

receiving a selection of one of the presented applications to be instantiated;

setting the chooser value to a value corresponding to the selected application;

transitioning from the normal mode to ~~re-entering~~ the preferred mode upon [[an]] a second non-power-up executed CPU reset after setting the chooser value to the value corresponding to the selected application, and thereafter again instantiating and running the security kernel while in the preferred mode, the security kernel determining that the chooser value corresponds to the selected application and therefore authenticating same, the selected application being instantiated by the security kernel while in the preferred mode and only after being authenticated;

transitioning from the preferred mode to ~~re-entering~~ the normal mode after the selected application is instantiated and leaving same to run while in the normal mode, the selected application as instantiated during the preferred mode being available for use during the transitioned-to normal mode;

wherein the security kernel allows the processor to be trusted to keep hidden a secret of the chooser application and a secret of the selected application~~, and~~

~~wherein the processor has a cache, the method further comprising:~~

~~erasing data in the cache of the processor when entering preferred mode such that any data previously stored in the cache is not available to interfere with preferred mode operations; and~~

~~erasing data in the cache of the processor when entering normal mode such that any sensitive data in the cache from preferred mode operations is not available during normal mode from such cache~~.

26. (Currently Amended) The method of claim 25 further comprising setting the chooser value to the value corresponding to the chooser application upon the selected application being authenticated by the security kernel, wherein upon execution of a CPU reset, the security kernel determines that the chooser value corresponds to the chooser application ~~72e~~ and therefore authenticates same.

27. (Original) The method of claim 25 further comprising storing the chooser value in a memory location not affected by a CPU reset so that the stored chooser value is available after same.

28.-30. (Canceled)

31. (Currently Amended) A computer-readable medium having stored thereon computer-executable instructions implementing a method for a secure processor to instantiate a secure application thereon by way of a security kernel, the method comprising:

powering on into a normal mode;

receiving an instruction to instantiate the application after being powered on and while being in the normal mode;

after receiving the instruction to instantiate the application, transitioning from the normal mode to ~~entering~~ a preferred mode upon a non-power-up executed CPU reset, where a security key of the processor is accessible while in the preferred mode;

instantiating and running a security kernel while in the preferred mode, the security kernel:

accessing the security key;

applying the accessed security key to decrypt at least one encrypted key for the application;

storing the decrypted key(s) in a location where the application will expect the key(s) to be found; and

authenticating the application on the processor;

instantiating the application while in the preferred mode and only after the security kernel has authenticated such application; and

transitioning from the preferred mode to the ~~entering a~~ normal mode ~~from the preferred mode~~ after the security kernel authenticates the application and the application has been instantiated, where the security key is not accessible while in the normal mode, the application as instantiated during the preferred mode being available for use during the transitioned-to normal mode;

wherein the security kernel allows the processor to be trusted to keep hidden the key(s) of the application, and

wherein the security kernel employs the accessed security key during the preferred mode to authenticate / verify the application prior to instantiation thereof~~,~~

~~wherein the processor has a cache, the method further comprising .~~

~~erasing data in the cache of the processor when entering preferred mode such that any data previously stored in the cache is not available to interfere with preferred mode operations; and~~

~~erasing data in the cache of the processor when entering normal mode such that any sensitive data in the cache from preferred mode operations is not available during normal mode from such cache~~.

32.-35. (Canceled)

36. (Previously Presented) The medium of claim 31 wherein the security kernel performs a hash / MAC (message authentication code) over at least a portion of the application and then compares the hash / MAC to a hash / MAC corresponding to the application.

37. (Original) The medium of claim 31 wherein the security key of the processor is a symmetric key and the application is instantiated from a code image including a main body and a header including:

KCPU (KMAN)	KMAN encrypted according to KCPU
KMAN (KCODE)	KCODE encrypted according to KMAN

where KCPU is the security key, KMAN is a device key of the portable device independent of the security key, and KCODE is the secret of the application, and

wherein the security kernel applying the accessed security key to decrypt at least one encrypted key for the application comprises:

applying KCPU to KCPU (KMAN) to produce KMAN; and

applying KMAN to KMAN (KCODE) to produce KCODE.

38. (Original) The medium of claim 37 wherein the security key of the processor is a symmetric key and the application is instantiated from a code image including a main body and a header including:

KCPU (KMAN)	KMAN encrypted according to KCPU
MAC (main body, KMAN)	message authentication code of the main body under KMAN
KMAN (KCODE)	KCODE encrypted according to KMAN

where KCPU is the security key, KMAN is a device key of the portable device independent of the security key, and KCODE is the secret of the application, and

wherein the security kernel applying the accessed security key to decrypt at least one encrypted key for the application comprises:

applying KCPU to KCPU (KMAN) to produce KMAN;

computing MAC (main body, KMAN);

comparing the computed MAC to MAC (main body, KMAN) from the header to determine if the code image has been changed; and

if the MACs match, applying KMAN to KMAN (KCODE) to produce KCODE.

39. (Original) The medium of claim 31 wherein the security key of the processor is a private key of a public key - private key pair and the application is instantiated from a code image including a main body and a header including:

public key (KCODE)	KCODE encrypted according to the public key

where KCODE is the secret of the application, and

wherein the security kernel applying the accessed security key to decrypt at least one encrypted key for the application comprises applying the security key as the private key to public key (KCODE) to produce KCODE.

40. (Original) The medium of claim 39 wherein the security key of the processor is a private key of a public key - private key pair and the application is instantiated from a code image including a main body and a header including:

public key (HASH (main body), KCODE)	Hash of the main body and KCODE, both encrypted according to the public key

where KCODE is the secret of the application, and

wherein the security kernel applying the accessed security key to decrypt at least one encrypted key for the application comprises:

computing HASH (main body);

applying the private key to public key (HASH (main body), KCODE) to produce HASH (main body) and KCODE;

comparing the computed HASH to the produced HASH to determine if the code image has been changed;; and

if the HASHs match, employing the produced KCODE as appropriate.

41. (Currently Amended) A computer-readable medium having computer-executable instructions thereon implementing a method for a secure processor to instantiate one of a plurality of available secure applications thereon by way of a security kernel, the method comprising:

setting a chooser value to a value corresponding to a chooser application upon power-up;

entering a preferred mode upon a first power-up CPU reset and instantiating and running the security kernel while in a preferred mode, the security kernel determining that the chooser value corresponds to the chooser application and therefore authenticating

same, the chooser application being instantiated by the security kernel while in the preferred mode and only after being authenticated;

transitioning from the preferred mode to a ~~entering a~~ normal mode after the chooser application is instantiated and leaving same to run while in the normal mode, the chooser application while in the normal mode presenting the plurality of available applications for selection by a user;

receiving a selection of one of the presented applications to be instantiated;

setting the chooser value to a value corresponding to the selected application;

transitioning from the normal mode to ~~re-entering~~ the preferred mode upon [[an]] a second non-power-up executed CPU reset after setting the chooser value to the value corresponding to the selected application, and thereafter again instantiating and running the security kernel while in the preferred mode, the security kernel determining that the chooser value corresponds to the selected application and therefore authenticating same, the selected application being instantiated by the security kernel while in the preferred mode and only after being authenticated;

transitioning from the preferred mode to ~~re-entering~~ the normal mode after the selected application is instantiated and leaving same to run while in the normal mode, the selected application as instantiated during the preferred mode being available for use during the transitioned-to normal mode;

wherein the security kernel allows the processor to be trusted to keep hidden a secret of the chooser application and a secret of the selected application~~, and~~

~~wherein the processor has a cache, the method further comprising:~~

~~erasing data in the cache of the processor when entering preferred mode such that any data previously stored in the cache is not available to interfere with preferred mode operations; and~~

~~erasing data in the cache of the processor when entering normal mode such that any sensitive data in the cache from preferred mode operations is not available during normal mode from such cache~~.

42. (Currently Amended) The medium of claim 41 wherein the method further comprises setting the chooser value to the value corresponding to the chooser

application upon the selected application being authenticated by the security kernel, wherein upon execution of a CPU reset, the security kernel determines that the chooser value corresponds to the chooser application ~~72c~~ and therefore authenticates same.

43. (Original) The medium of claim 41 wherein the method further comprises storing the chooser value in a memory location not affected by a CPU reset so that the stored chooser value is available after same.

44.-46. (Canceled)